DCS3101
Assignment 3

Kent Odde

October 31, 2020

Contents

Abstract

This is my submission for the third compulsory assignment in DCS3101, Introduction to Cybersecurity.

Q1

> *What are the advantages of firewalls?*

A firewall is a component, that functions as a check-point in a network, and its job is to monitor and regulate traffic passing through it.

The main use case and advantage of a firewall, is that we can protect a local trusted network against threats which might exist on another untrusted network.

When implemented, all traffic passing from network A to network B must pass through the firewall. The firewall may prohibit traffic it considers a threat. This decision has traditionally been based on a predefined ruleset, but next-generation firewalls have much more sophisticated methods of identifying potential threats.

A strength of firewalls is their wide range of types suitable for different needs, and their capability for configuration. We can have an open firewall, where we define rules for what the firewall should filter out, or for a more conservative approach, we can have a firewall which filters all packages, and we whitelist the traffic we do want.

We can filter traffic based the sender or receiver or by the contents of the packets, which can be used to protect specific hosts or specific ports. We can filter based on the types of application layer protocol the package contains, which can help us filter out spam mail etc. We can also use the TCP headers, so that an outgoing TCP packet on a port, will temporarily open the port for incoming packets, given that the TCP header contain the correct information.

There are also *next-generation* firewalls, which can employ machine learning to be able to recognize unknown types of malicous traffic based on patterns.

As an added bonus of all this, we can also configure firewalls to log all traffic, which may be very handy for several reasons, but especially if we find out that our network has been compromised.

Q2

Comment if the following is true or false in the context of TLS - "The algorithms inside a session are negotiated between client and server." Justify your answer with an associated protocol diagram.

The statement in the question is **true**. Different clients and servers will have support for different encryption and MAC algorithms. Just like different people speak different languages. The goal of the negotiation is to find mutually supported algorithms, that are also recognized as secure enough by the current version of TLS.

However, negotiation is perhaps a strong word. If we look at subset of the TLS handshake protocol in figure 1, we can see that the client starts the conversation with a *hello*.

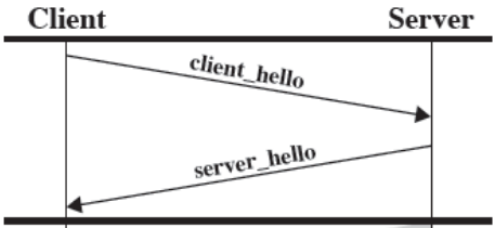

Figure 1: Part of the TLS handshake protocol diagram from lecture

This hello consists of information about the client, like what algorithms it has support for. One of the things the server then does, is to pick the strongest of these algorithms that it self supports. The server hello will then among other things, contain this decision.

Q3

It was discussed in the class about one particular attack on TLS. Discuss this attack and identify another attack that can impact TLS. Discuss briefly about the attack you have chosen for your answer.

The attack discussed in class was the exploitation of what has come to be known as the *heartbleed bug*. This was a bug in the heartbeat protocol of TLS.

The heartbeat protocol, is a mechanism for letting the client check that the connection with the server is still active. The client would send a message asking for a distinct string as a reply, and the character length of this string. If the connection was still alive, the server would naturally send the requested string back.

However, it was discoverd that if the number containing the length of the string was much higher than the actual length of the string, the server would in addition to the string send random content of its RAM. This was of course catastrophic, as a web-servers RAM is filled with a lot of information that can be exploited, like encryption keys and so on.

When it comes to other TLS vulnerabilites, there are plenty to choose from. They can be categorized into whether they arise from a flaw in the initial concept of TLS, the implementation, etc. Since heartbleed can be categorized as an implementation bug, I have chosen to write about a concept flaw.

FREAK

Freak is an acronym, and means *Factoring RSA Export Keys*. In the 1990's computing power was scarce among the general public, and encryption did not have to be very strong to still be reckoned as secure. Previous to this, the American government had put a ban on the export of strong cryptographic technology, limiting applications meant for export to use RSA with a maximum of 512 bits. The upside to this was that the NSA was able to break these ciphers, but in essence, nobody else would.

However, throughout the 2000's computing power became more widespread. This meant that in essence, anybody would be able to break them. Luckily the cryptographic export laws were abolished in 2000, so by this time, most applications had moved on to stronger encryption.

The Freak attack however, made use of the fact that encryption of export grade were still available in a lot of applications and on a lot of servers. This allowed for a man in the middle, to trick clients to use weaker cryptographic schemes,

and then easily decrypt the information sent.

This attack is no longer possible in TLS 1.3, as it no longer allows for a downgrade to the weaker protocols.

Q4

What are the differences between IDS and IPS? Discuss on classification/taxonomy of IDS and IPS.

In order to see the differences more easily, lets start with looking at the similarities.

Intrusion Detection Systems and Intrusion Prevention Systems are both constructs i the network infrastructure. They will analyze packets in the network, and in various ways check whether or not the packet is deemed as a threat. This is most commonly done by comparing the packet with the contents of a database, storing known malicious threats.

The main difference however is that while they both monitor the network and try to detect threats, an IPS will also prevent malicious packets from entering the internal network. In other words they live more in the domain of firewalls.

IDS can be separated into two main categories, based on the implementation:

- **Host Instrusion Detection**
  Individual host implementation. Dependent on the logs within the host. May take up a lot of resources on the host.
- **Network Intrusion Dectection System**
  Monitors traffic on the network, to and from all hosts. It is easy to implement.

However, we can also categorize them based on their method of threat detection:

- **Signature-based Intrusion Detection Systems**
  Looks for specific bit sequences in the packet payload, which has been flagged as a possible threat. Can not detect new threats.
- **Anomaly-based Intrusion Detection Systems**
  The system uses training data, to learn what is deemed as *normal* traffic, and then it looks for packets which deviate from the norm to a certian degree.

As far as I could find, IPS is also classified by the same categories as IDS, as it of course has a detection system within. I could unfortunately not find any categories or differences of how the actual prevention is done.

Q5

Biometrics - What are the key factors for choosing a biometric modality (e.g., face, fingerprint, iris, etc)?

As with every other choice, the decision of which biometric modality to use depends on the particular use case.

If one is dependent on extremely robust security, the best choice will differ than if they key factor was user conveniance and security was second priority.

The metrics of modalities as mentioned in the lectures are great ways for making this decision:

- Failure-to-Capture Rate
- Failure-to-Extract Rate
- Failure-to-Enrol Rate
- Failure to Acquire Rate
- False-Match-Rate
- False-Non-Match Rate

The first four points are very important if the goal is user conveniance, as a lot of failures of creating and storing a template will result in irritation. However, if the key goal is security, high numbers here may be acceptable.

The two last points will be a trade off between usability and security. If the false match rate is virtually zero, the false non match rate will probably be higher. As no system is perfect, this will be a choice depending on how critical security is.

Q6

What kind of attacks are possible on face biometric systems?

Face biometric systems may be succeptible to several attacks, based on the sophistocation of the implementation.

The most obvious one is of course just threatening the person to which a face belongs, to unlock the system. However, this sort of attack is not very sophisticated, carries great risk, and is quite rare.

Among the more realistic attacks, they all revolve around simulating the face in some way. These are often called presentation attacks.

You can have a photograph of a face, a video of a face or various types of masks.

Whether or not these work, depend on the implementation. To combat them one may use sensors or 3D-cameras to make sure that there is in fact a person present. One may also use particular expressions or movements in the face when storing the template.

There are also more classical attacks, that apply for all sorts of security, where one tries to access the system, and manipulate the template database or weaken the match acceptance criteria.

References

[1] FREAK, wikipedia. https://usn.instructure.com/courses/22192/files/folder/Slides-Compact-Version? Accessed: Oct-20.

[2] Lecture slides, canvas. https://usn.instructure.com/courses/22192/files/folder/Slides-Compact-Version? Accessed: Oct-20.

[3] Towards Data Science, facial recognition attacks. http://pi.math.cornell.edu/~mec/2003-2004/cryptography/subs/frequencies.html. Accessed: Oct-20.